BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images,
Please do not report the images to the
Image Problem Mailbox.

Ins: a1

TITLE

COPY PROTECTION SYSTEM FOR PORTABLE STORAGE MEDIA

CLAIM FOR PRIORITY

This application makes reference to, incorporates the same herein, and claims all rights accruing thereto under 35 U.S.C. §119 through our patent applications entitled *The Digital Content Encryption Apparatus And Method Thereof* earlier filed on the 24th day of September 1998 in the Korean Industrial Property Office and there duly assigned Serial Nos. 1998/39808 and 1998/39809.

FIELD OF THE INVENTION

The present invention is generally related to encryption processes and apparatus, and, more particularly, to secure and robust processes and apparatus for the generation and use of keys in the transmission and replay of digital information for licensed SDMI compliant modules such as personal computers and SDMI compliant portable devices in conjunction with Internet service content provider and certificate authority.

BACKGROUND ART

Recently, with the flood of information provided by various media such as broadcasting and press, an atmosphere has been created by the information providers who are interested in providing integrated information that covers all of the media. Other users want to selectively receive a specific

item of digital information from the entire spectrum of information available from a particular information provider (IP). Accordingly, a digital content transmission system has been formed by the information providers who convert various types of information into digital form and store this digital information, and the users who subscribe to this digital information system from the information provider via the network. Digital information transmission systems endow an application program with easy downloadability of the digital content. The user can get all the information desired by using this application program to access the digital information system through the network.

The digital information may be provided to the user either for pay or for free. In case of paid digital information, the server who provide the digital information via the transmission system sets the service fee. The service server charges the user according to the quantity of information used when the digital information is downloaded to the user. MPEG software protocol for example, compresses audio files to a fraction of their original size, but has little perceptible affect upon the quality of the audio sound. MPEG software protocol is now widely used by Internet sites offering digitalized music, and is reported to be commonly used to offer digitalized versions of recorded music without the consent of the musicians. When a user is connected to a server that provides digital information commercially via a network, a few of the users may be able to inadvertently or illegally copy the digital information, a practice that, as was recently noted by Interdeposit and the French Agency for the Protection of Programs, a member of the European Association of Authors and Information Technology Professional, in the *Patent, Trademark & Copyright Journal*, volume 57, No. 1416, page 385 (11 March 1999), would be economically damaging to both the musicians

and to the server who is running the digital information transmission system. Currently, the server, as well as the musicians, can do little more than seek redress by undertaking civil and criminal action in an effort to control the possibility of unlicensed reception of digital information. We have noticed that there is a need for a technique to preserve transmission security of revenue bearing information while restricting access to the information by unauthorized entities and preventing unauthorized users from using any of the information that they may be able to illicitly obtain from the information provider by restricting the ability of the unauthorized users to decrypting whatever information they manage to obtain via the system.

SUMMARY OF THE INVENTION

It is therefore, one object of the present invention to provide improvements in cryptographic processes and apparatus.

It is another object to provide a secure and robust digital encryption process and apparatus.

It is yet another object to provide digital encryption processes and apparatus endowing a system with secure and robust copy protection for LCM's (*i.e.*, licensed SDMI (*i.e.*, secure digital music initiative) compliant modules such as personal computers) and PD's (*i.e.*, SDMI compliant portable devices such as disk and DVD players) in conjunction with ISP (*i.e.*, Internet service provider) and CA (*i.e.*, certificate authority).

It is still another object to provide digital encryption processes and apparatus able to encrypt and transmit digital information received from a transmission system, by the use of multiple cryptographic keys.

It is still yet another object to provide digital encryption processes and apparatus for generating and using multiple cryptographic keys during the transmission of digital information to a user.

It is a further object to provide digital encryption processes and apparatus that employ user information in the generation and use of multiple cryptographic keys during the transmission of digital information to the user.

It is a yet further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using multiple cryptographic keys, and to decrypt and play the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

It is a still further object to provide digital encryption processes and apparatus able to encrypt and transmit digital information obtained from a transmission system by using key information, a user's key, and a temporary validation key, and to decrypt and play the digital information at the terminal of the user by using the key information and user authorization information.

It is still yet a further object to provide encryption, transmission and reception protocols enabling encryption, transmission and decryption of digital information received from a transmission system.

It is an additional object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system by using multiple keys to encrypt the digital information, and decryption and replay of the digital information at the terminal of the user by using a plurality of keys, one of which is common to the multiple keys.

It is a still yet further object to provide encryption, transmission and reception protocols enabling encryption and transmission of digital information received from a transmission system, by using key information, a user's key, and a temporary validation key, and decryption and replay of the digital information at the terminal of the user by using the key information and user authorization information.

It is also an object to provide a more secure cryptograph and process for transmitting information to a terminal of a user who has requested the information.

It is also a further object to provide a cryptograph and process that reliably restricts the ability of a registered subscriber who has validly obtained information from an information provider, to deliver that information to another entity in a readily usable form.

These and other objects may be attained with an encryption process and apparatus that provides a secure and robust copy protection system for a licensed secure digital music initiative compliant modules such as personal computers and portable devices, in conjunction with Internet service providers and certificate authorities, by responding to a user's request for transmission of items of digital information to the user's terminal unit, by providing copy protection during downloading and during uploading of the digital contents. In order to prevent the digital contents from being copied illegally, a plurality of keys are generated and held by both the user and the digital content provider, and a secret channel is formed between both the user and the digital content provider. The header of the encrypted digital content is encrypted by using a physical address of a sector of a licensed SDMI compliant module such as a portable computer or a portable media device in order to prevent the digital content from being copied illegally after the digital content is recorded

in the portable media.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of this invention, and many of the attendant advantages thereof, will be readily apparent as the same becomes better understood by reference to the following detailed description when considered in conjunction with the accompanying drawings in which like reference symbols indicate the same or similar components, wherein:

Fig. 1 is a block diagram illustrating the overall architecture of an implementation of the principles of the present invention;

Fig. 2 is a block diagram illustrating a registration by an original equipment manufacture of a portable device with a certificate authority;

Fig. 3 is a block diagram showing the registration of a Internet service provider's registration with a certificate authority;

Fig. 4 is a block diagram showing the registration of a personal computer and a portable device with an Internet service provider;

Fig. 5 is a block diagram showing usage rules governing a database of a right management system;

Fig. 6 is an exemplified format;

Fig. 7 is a block diagram showing the basic architecture for various inputs;

Fig. 8 is a block diagram showing control of outsource import; and

Fig. 9 is a block diagram showing a copy protection system for portable media.

PATENT
P55690

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

1. INTRODUCTION

In this manuscript we describe, as Samsung's proposal for the SDMI standardization, the specific roles and processing rules of the LCM (Licensed SDMI Compliant Module, e.g. personal PC) and SDMI Compliant Portable Device (PD).
First, in section 2, we depict our total architecture for a secure Electronic Music Distribution (EMD) as a candidate for the SDMI Compliant EMD. In section 3, for the removal of the ambiguities on some terminologies and for the clear explanation of our proposal, some terminologies are defined. For some basic requirements or basic modules to be preset within LCM or PD for their secure installation and secure content transaction are presented in section 4 and the initialization protocol of LCM and PD is described in section 5. From section 6 to section 8, the secure content transaction protocol over ISP-LCM-PD-PM are described via the appropriate file format appeared in section 7 and using some functional roles facilitated by those in section 6. Furthermore, our proposed SDMI compliant processes for the considerable various outsource inputs to LCM or PD is presented in section 9.

2. OUR OVERALL ARCHITECTURE

In our overall architecture depicted in the following, the ISP (Internet Service(Content) Provider) and PD-Manufacturer should register to CA(Certificate Authority, e.g. SDMI) to achieve their right certificate for SDMI Compliant Role or Product. When an ISP registers to CA, CA issues a certificate to the ISP's Public Key and stores it into its Data Base and hereafter helps a LCM to makes use of this data to authenticate the ISP when it needs to register to the ISP. And when a PD-Manufacturer registers to CA, CA also issues a manufacturer key and its certificate for the manufacturer and stores it into its Data Base and hereafter, by use of this, stipulates a secure PD-Registration to a LCM by checking its certificate validation in the LCM and by constructing a secure channel between them. Note that any ISPs do not have any knowledge about the manufacturers' keys.
While some content transfer between LCM and PD occurs, the right management system may act on the header part of its file format, where, of course, each communication or content transaction among the members appeared in the Fig.2-1 should be done only after their authenticating and constructing a secure channel. As for the right management of contents, our proposal contains Copyright Status, Playback Status, and Transfer Status. In our proposal, the transferability of a content is discriminated from the portability of it. The Kiosk-like machine is to be treated as a LCM, but is to be subject to the groups of copyright holders.

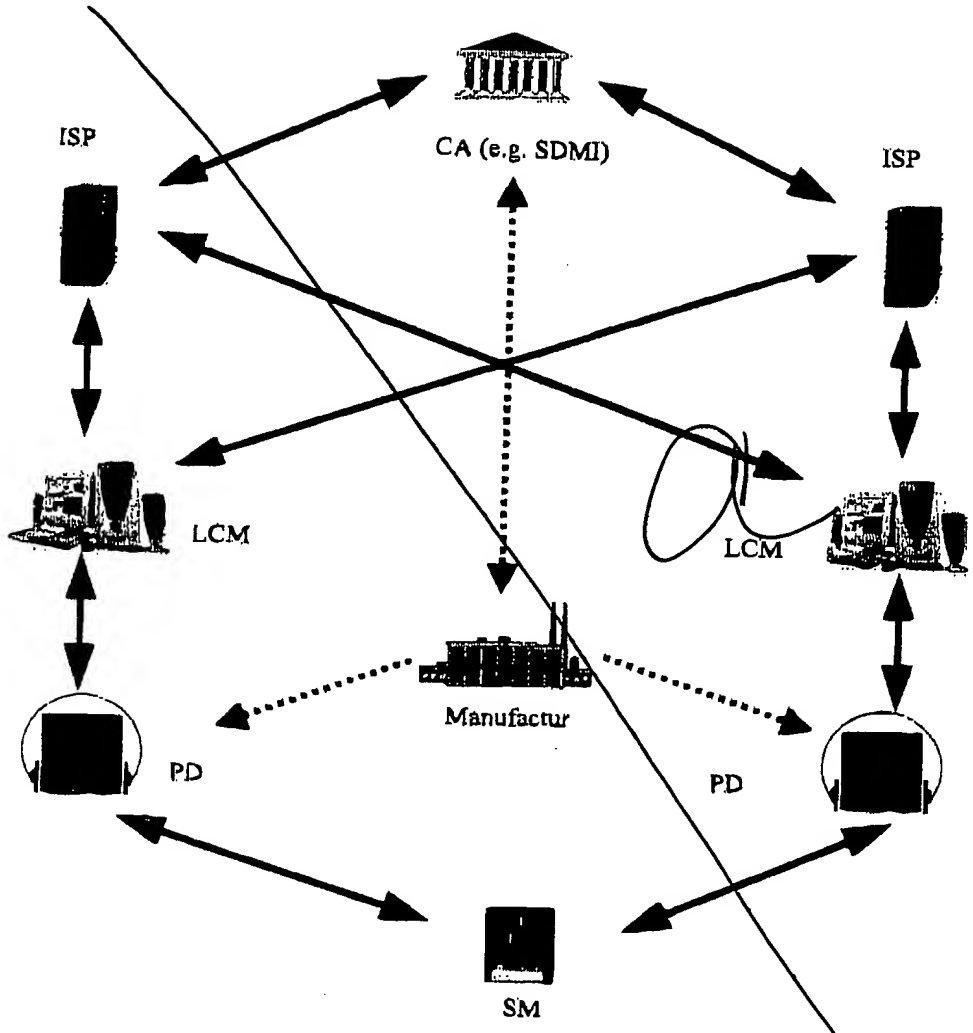


Figure 5-1 : The Overall Architecture

3. SOME TERMINOLOGIES

For the removal of some ambiguities, in this section, we define some terminologies and list up some abbreviated words for a simple description (most of them are those commonly used in PDWG).
First, we have to distinguish the two words, "Portability" and "Transferability" of a content.

- **Portability** – a content in a PM can be played in *any PD*
- **Transferability** – Portability + "upload of a content is allowed from a PM to even a LCM", in this case the content's uploadability is to be controlled by *check-in/out system* and its *transferability status*.

Hereafter we use the following abbreviated words.

- **CA** – Certificate Authority (e.g. SDMI, or other trust third party)
- **LCM** – Licensed SDMI Compliant Module
- **PD** – SDMI Compliant Portable Device
- **PDFM** – Portable Device Functional Module

- **ISP** – Internet Service Provider (including Content Provider via the Internet)
- **PM** – Portable Media (SDMI Compliant Storage Media)

Furthermore, here are presented some notations to be used in the following sections. Even though they are some intricate, we are sure that they would help the readers clearly understand the concrete method we intend. They are relevant to the algorithmic functional modules.

- **ECC** – Elliptic Curve Cryptosystem
- $\mathbf{PrvKey_A}$, $\mathbf{PubKey_A}$ – Private Key and Public Key of A (this may be LCM, PD (optional), ISP, CA, ...) , respectively.
- $\mathbf{Cert_{CA}(PubKey_A)}$ – A Certificate for a Public Key $\mathbf{PubKey_A}$ issued by **CA**.
- $\mathbf{MK_{PD}}$ – The Manufacturer Key within a PD
- $\mathbf{ID_{MK}}$ – The Indicator of a Manufacturer Key
- $\mathbf{CK_{PD\text{-}LCM}}$ – This is a secure (secrete) channel key which is setup between PD and LCM
- **EC_ENC(*key* , *C*)** – Elliptic Curve Encryption of a content *C* by utilizing a public key, *key*. *Where the encryption is the ElGamal-like public key encryption process. And Samsung can support its own ECC implementation technique that is very effective for both S/W and H/W implementation.*
- **EC_DEC(*key* , *C*)** – Elliptic Curve based Decryption of a ciphertext (encrypted text) *C* by utilizing a private key, *key*.
- **EC_DH(*A*, *B*)** – A random secret value (key) shared between *A* and *B* by Elliptic Curve based Diffie-Hellman Key Exchanging Protocol.
- **ENC(*key* , *C*)** - Symmetric Key Encryption of a content C by utilizing a secrete key, *key*. *Samsung can support its own Symmetric Key Encryption algorithm, named "**SNAKE**", that is very effective for both S/W and H/W implementation and it has been world-wide cryptanalized.*
- **DEC(*key* , *C*)** – Symmetric Key Decryption of a ciphertext *C* by utilizing a secrete key, *key*.

Note: In the above items the Elliptic Curve based Public Key Cryptosystem is just an example as a candidate of Public Key Cryptosystem, and so any public key cryptosystem, for example RSA, can be used instead of it. But we suggest that SDMI Compliant EMD System (Electronic Music Distributing System) adopt the ECC System for the next generation PDs, since ECC can be efficiently implemented in such small devices with low cost.

4. BASIC REQUIREMENTS FOR THE SECURE SETUP OF LCM AND PD

Here we present the minimum substances (algorithms) that are needed for the insurance of the security of LCM and PD. It is assumed that the content compressing and decompressing CODECs are built in each device in either S/W-form or H/W-form.

4.1. For the LCM

- **Public Key Cryptosystem (PKC)** – ECC, RSA, ... (*ECC is more preferable*)
  → This is to be used for the secure key setup of LCM, the validity check of ISP's Public Key Certificate, and the secure channel construction between ISP and LCM.
- **Symmetric Key Encryption Algorithm** – SNAKE, ...
  → This is to be used for the content encryption, the authentication to a PD, and the secure channel construction between LCM and PD.
- **Secure Check-in/Check-out System** – It is to be presented in section 6, 7 how to construct this system and how to securely maintain it.

4.2. For the PD

- **Public Key Cryptosystem (PKC)** – Optional to PD.
- **Symmetric Key Encryption Algorithm** – SNAKE, ...
  → This is to be used for the content encryption, the authentication to a LCM, and the secure channel construction between PD and LCM.
- **Manufacturer Key, $\mathbf{MK_{PD}}$** – the pre-set manufacturer key in a temper resistant area within the PD.

→ This is to be used for the secure registration of a PD to LCM.

4.3. For the PM

There needs an apparatus or a pre-set special information within a PM to protect contents in it from the dead-copy to another PM. It is desirable, we think, to use the unique ID based approach, that is the method that the manufacturers of PM imbed a unique ID of each PM in the write-protected area of it while they manufacture it. This can be considered as a low cost method to dead-copy protection for the 1st generation PM.

5. INITIALIZATION (KEY SETUP) MECHANISM

There are 4 registration mechanisms relative to ISPs, LCMs, and PDs. The manufacturers' registration to CA is preceded ahead all the others.

5.1. Registration of PD manufacturers to CA

Prior to manufacturing PD, the manufacturers should register to CA to get their manufacturer key, $\mathbf{MK_{PD}}$, and its certificate, $\mathbf{Cert_{CA}(ID_{MK})}$, and then produce the SDMI Compliant Portable Devices by using them. Where such registered manufacturer keys are securely stored in CA's DB and only CA maintains the information. The manufacturer should keep their manufacturer-key and its certificate in safe, maintain it securely, and imbed them in a temper resistant area of PDs while he manufactures PDs. In the Fig.5.1-1 an illustrated example is depicted.

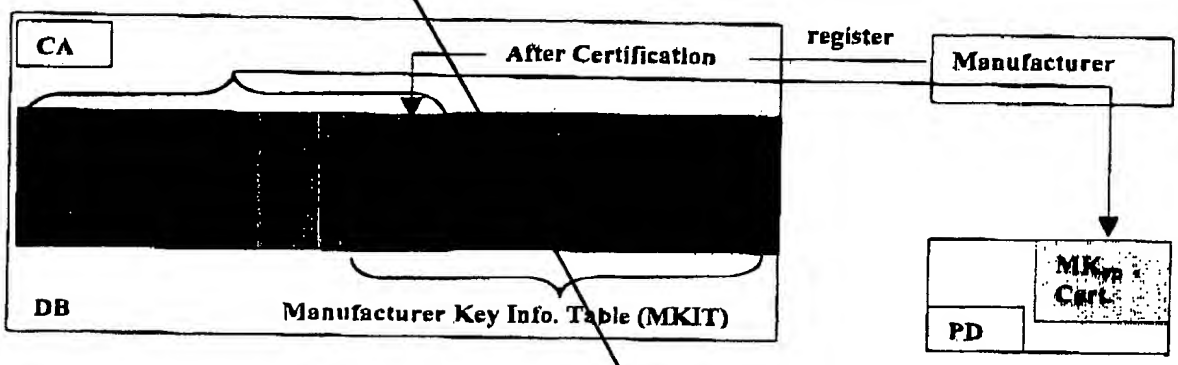


Figure 5.1-1: PD-Manufacturer's Registration to CA

In this figure, when a manufacturer request its registration to CA, CA certifies it and then generates a manufacturer key, MK_{PD}, and make its certificate data, $Cert_{CA}(ID_{MK})$, to deliver them to the manufacturer. At the same time CA generates a random token, T, to make (or update) the Manufacturer Key Information Table (MKIT) for the other ISP-registration. Once after a manufacturer got the data, $\{MK_{PD}, Cert_{CA}(ID_{MK})\}$, he/she can manufactures PDs by imbedding those secrete data within a temper resistant area of PDs.

5.2. Registration of ISP to CA

The following Fig.5.2-1 shows how for an ISP to register to CA and what information to get from CA. For an ISP to register to CA, firstly it generates its ephemeral private-public key pair $\{PrvKey_{eph}, PubKey_{eph}\}$ to open a secure channel between CA and itself by **EC_DH(CA, ISP)**. Secondly the ISP gets its semi-permanent private-public key pair $\{PrvKey_{ISP}, PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ and MKIT data appeared in Fig.5.1-1 through the secure channel. Where CA's certification to the ISP should be preceded ahead all these procedures.

Note : ISP's Key Pair should be securely stored.

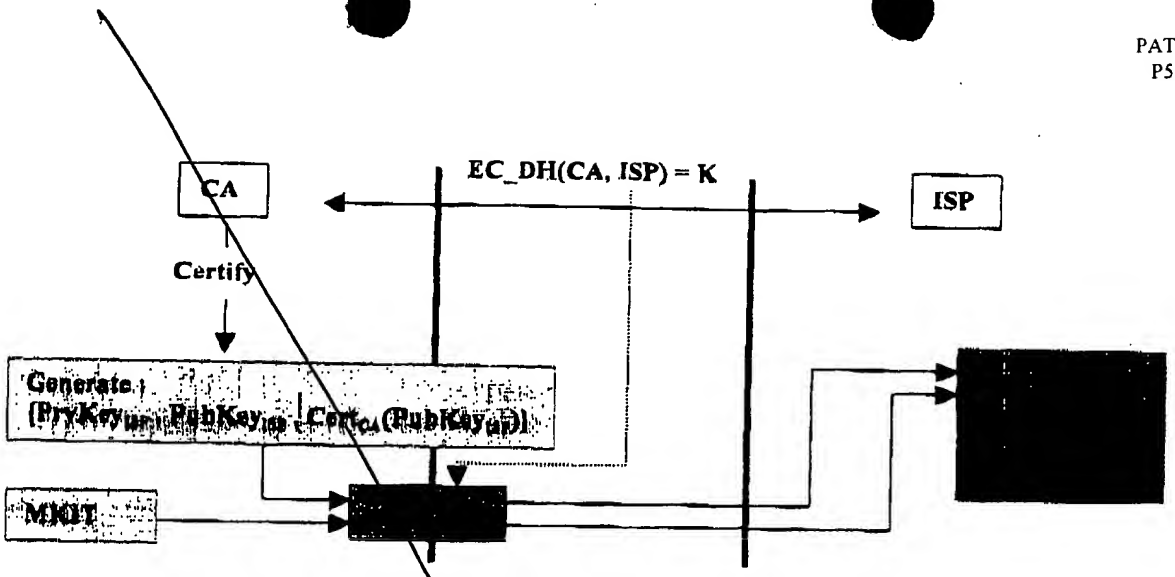


Figure 5.2-1 : ISP Registration to CA

Note : The LCM's Key Pair should be securely stored, where the host's various system parameters may be used for this goal.

5.3. Registrations of LCM to ISP and of PD to LCM

Here the LCM registration mechanism to an ISP together with PD registration is described. As in the Fig.5.3-1 LCM gets the ISP's Public Key Information $\{PubKey_{ISP}, Cert_{CA}(PubKey_{ISP})\}$ at first and verifies its validity by using the CA's Public Key Information which was already announced or preset within the LCM in a code-imbedded-like method.

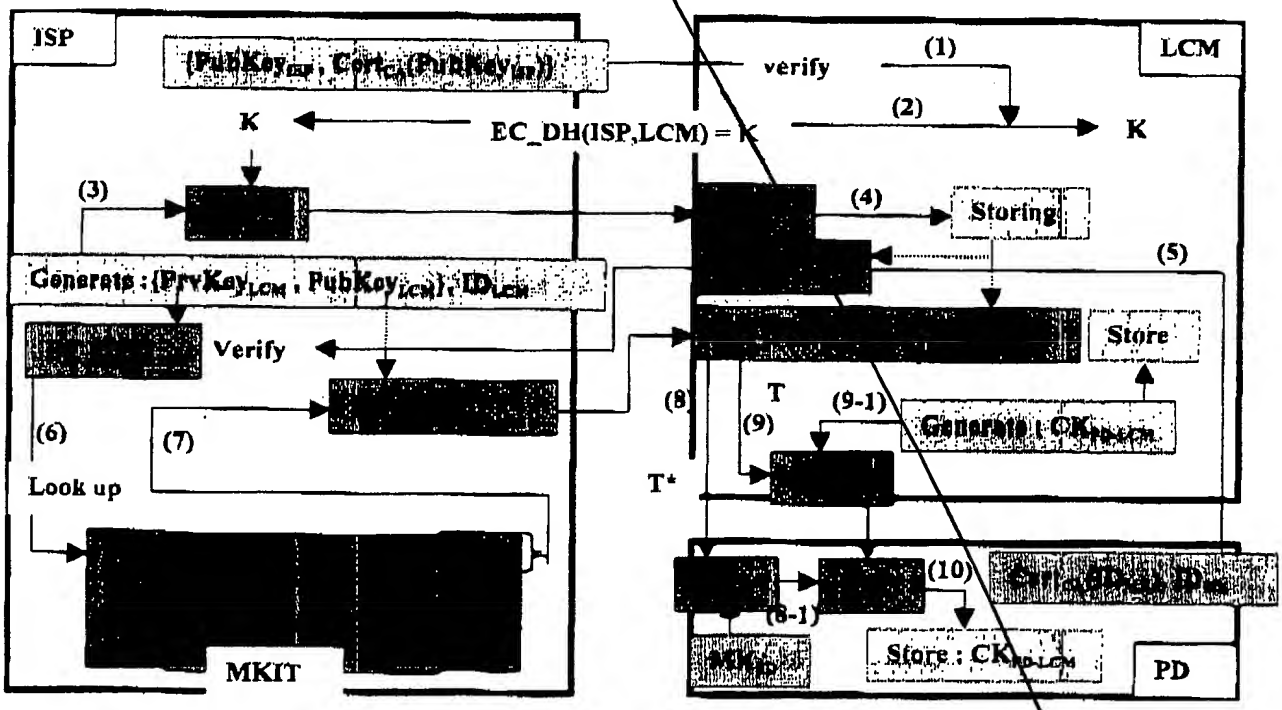


Figure 5.3-1 : LCM and/or PD Registration to ISP

If the validity of the certificate for the ISP's Public Key is certified, the LCM executes the handshaking protocol to get a ephemeral shared key by utilizing Elliptic Curve based (or other PKC based) Key Exchanging Protocol. Through this secure channel the ISP can deliver in safe the LCM's permanent private-public key pair for a static secure communication and a secure content transaction between the LCM and the ISP. For a PD to register to the LCM, it has to toss the certificate data for its ID of manufacturer key and the LCM gets this data from the PD to send this to its connected ISP in the encrypted form, $\mathbf{EC\_ENC(PubKey_{ISP}, Cert_{CA}(ID_{MK}))}$.
Using this, the ISP can verifies the manufacturer key information and can extract its relevant data, T*||T by looking up MKIP in ISP's DB to transfer it to the LCM in secure manner, i.e. by $\mathbf{EC\_ENC(PubKey_{LCM}}$, $\mathbf{T^*||T)}$. For the LCM and the PD to setup a shared secrete key and to complete the PD registration, the LCM randomly generates their static and secret channel key $CK_{PD\text{-}LCM}$ and sends $\mathbf{ENC(\ T,\ CK_{PD\text{-}LCM}\ )||\ T^*}$. Upon receiving this data, the PD can extract the token value T from T* and using this token the PD can also compute $\mathbf{CK_{PD\text{-}LCM}}$. As the PD securely stores this channel key the PD-registration is finished.

Note1 : The Channel Key $CK_{PD\text{-}LCM}$ may be originated from PD instead of LCM. In this case the PD receives the data T* from the LCM and gets the token T by decrypting T* with its manufacturer key. And then the PD generates a random channel key $CK_{PD\text{-}LCM}$ to upload ENC(T, $CK_{PD\text{-}LCM}$) to LCM.

Note2 : The part of the record in MKIT (in LCM) stays in encrypted form by using the LCM's secrete key (this key may be LCM's Public Key).

Note3 : In practice, during the PD registration to LCM, the RMS-DB updating token data (UTD, appeared in section 6.1) should be transferred from the PD to LCM(or from the LCM to PD) together with $CK_{PD\text{-}LCM}$ and be set both in the RMS-DB and in the PD.

5.4. Registration of Multiple LCMs or Multiple PDs

Our architecture and the file format can allow users to register their own limited number of LCMs or PDs. The number may be limited by ISP or by CA.

- Registration of Multiple LCMs → since ISP maintains the private-public key pair of the firstly registered LCM of an user's multiple LCMs, ISP can securely deliver the same key pair to the another LCM of the user's.
- Registration of Multiple PDs → since LCM securely maintains the secret channel key between the LCM and PD, the LCM can securely deliver the same key pair to the another PD of the user's in the same manner depicted in Fig. 5.3-1.

6. COMPONENTS WITHIN LCM AND PD

6.1. Functional Components in LCM

- **Right Management System**
  → To manage the information CTC={Copyright, Transfer, Check-in/Check-out}, LCM has to maintain the Right Management System DB, named RMS-DB in a secure manner. Here we propose our secure Right Management System. In this system we focus on the content transaction between LCM and PD.
  The RMS-DB consists of the Title (or Title-ID), CTC field, Playback Control Status (PCS : the permitted times to play, the amnesty period, ...) and Update Token Data (UTD). This DB stays in LCM in the encrypted form by utilizing LCM's secrete key. An important characteristic of the Update Token Data (UTD) is that it is generated from PD whenever any content downloading or uploading session between PD and LCM occurs and that it is also stored in the PD.
  Whenever a content is played back at first in LCM, the above right management information of the content's file format is newly registered to the RMS-DB. Once a content is registered to the RMS-DB, every playback procedure should priory reference to the DB to check the content's validation. The following Fig.6.1-1 shows exemplified implementation for the management rule of RMS-DB when a content downloading occurs.

Note1 : The part of the record in RMS-DB (in LCM) stays in encrypted form by using the LCM's secrete key (this key may be $CK_{PD\text{-}LCM}$).

Note1 : The UTD part may have a few number of Updating Token Data depending on the number of a user's own PDs.

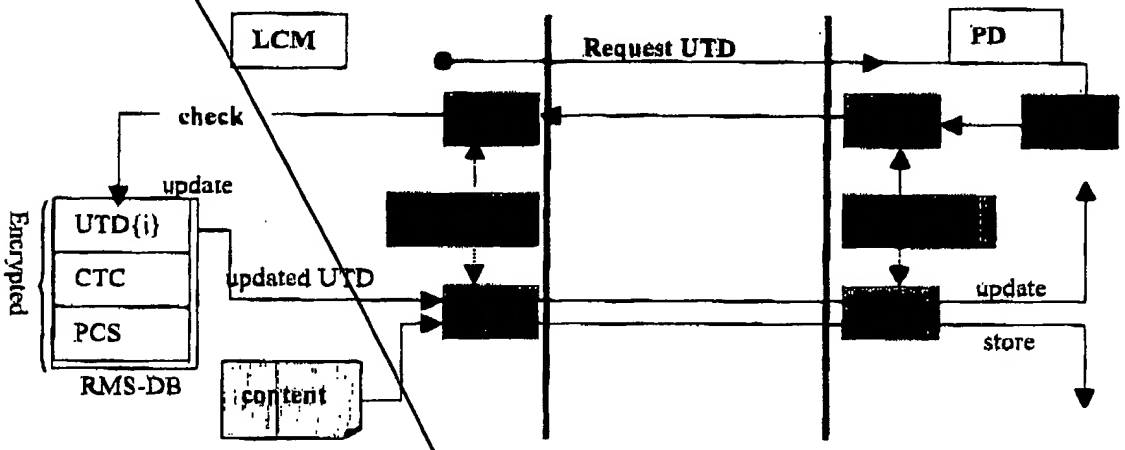


Figure 6.1-1 : Usage Rule of RMS-DB

Note : The RMS-DB may maintain a finite number of UTDs depending on the limited number of users' own PDs which were already registered to the LCM.

- **PD Import Control**
  This layer exists in LCM to import SDMI Compliant contents from ISPs or to import non-SDMI Compliant outsource contents (,e.g. RedBook CDs, DVD, ...). And so this should contain such capabilities as the followings.
  - Trans-Coding → to make PD decompress the input with its CODEC
  - Trans-Encrypting → to make PD decrypt the input with its Encryption System
  - Converting the input to SDMI Compliant file format

- **PD Interface**
  This has the following capabilities.
  - Authenticating to PD
  - Opening a secure channel between LCM and PD

- **ISP Interface**
  This has the following capabilities.
  - Authenticating to PD
  - Opening a secure channel between LCM and PD

6.2. Functional Components in PDFM

- **LCM Interface**
  This has the following capabilities.
  - Authenticating to LCM
  - Opening a secure channel between PD and LCM

- **Import Control within PDFM**

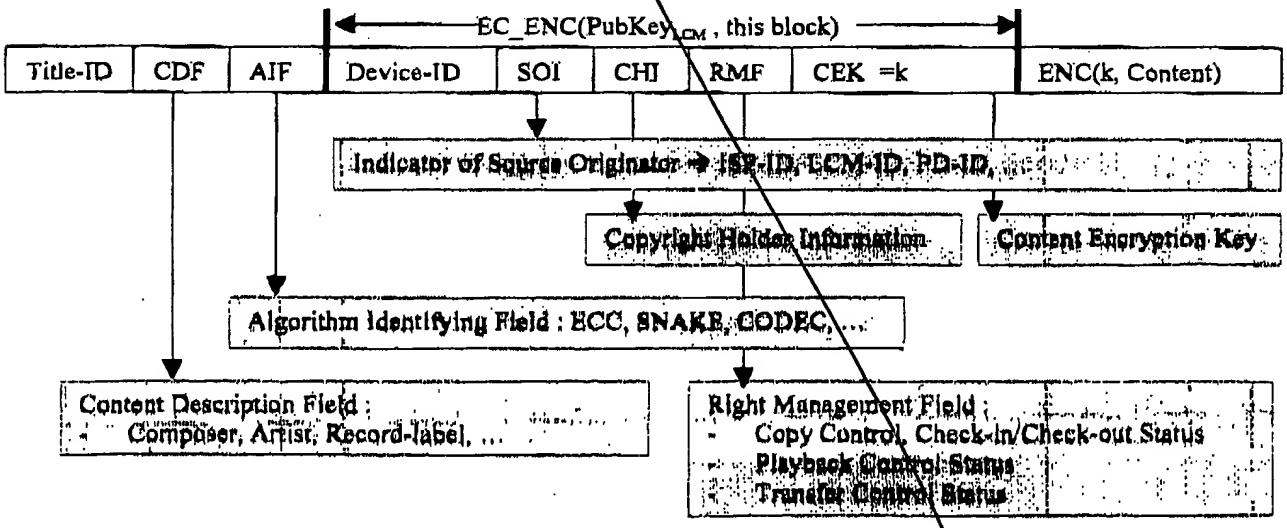
This has the capability to import a outsource analog input and to make it fit to the SDMI Compliant file format. Where the converted SDMI Compliant content should have the binding information to the PD to be played only via the PD.

7. SDMI COMPLIANT FILE FORMAT

The SDMI-Compliant file format should contain the following information and should allow extendibility and flexibility.

- Indication of Source Originator → ISP, LCM (CD-ripping, Audio input), PD (Analog input), Kiosk, ...
- Device IDentifier → LCM_ID, PD_ID, PM_ID
- Algorithm Information Field
  - ✓ Authentication secret sharing algorithm identifier → EC(Elliptic Curve)-Signature, EC-DH, ...
  - ✓ Encryption algorithm identifier → SNAKE, ...
  - ✓ Codec algorithm identifier → MP3, AAC, ...
  - ✓ Encryption key information of content
- Right Management Field
  Right management field contains the Copy, Check-In/Out, Transfer and Playback Control Status, which are to be encrypted by secret key of the device.
  - ✓ Copy-Never/Copy-Free/No-More-Copy mode
  - ✓ Check-In/Out mode
  - ✓ Transfer mode (Transferable or not)
  - ✓ Playback Control information
    - Allowable number of times to be played (unlimited or n-times)
    - Expiration date
    - Amnesty period
- Copyright holder information
- Content description field → Title, Composer, Artist, Record-label, ...

Here is illustrated an exemplified file format



We divide the above file format into the following three parts and we call them as in the following.

- Plain-Header (PH) – {Title-ID, CDF, AIF}
- Secret Header (SH) – {Device-ID, SOI, CHI, RMF, Content Encryption Key}
- File Body (FB) – {The Encrypted Content by using the content encryption key in SH}

8. SECURE CONTENTS TRANSACTION RULE OVER ISP-LCM-PD-PM

8.1. Contents Transaction from ISP to LCM

When an ISP receives a content downloading request from a LCM, it confirms the LCM's ID and then downloads the content with the file format of section 7 to the LCM. For the LCM to play the reached content, it follows the below steps in this order:

- Finding out the encryption algorithm from the field AIF in PH
- Using the found out encryption algorithm and LCM's secrete key (private key) to recover the fields in SH
- Comparing the Device-ID field with its ID
- From the RMF information confirming the Copy Control Status, Playback Control Status, and Transfer Control Status to register it to its RMS-DB
- Recovering the content encryption key from CEK to recover the real content from FB
- If any of the above lists does not violate, paying the music.

If it is needed to modify the RMF field, especially the Playback Control Status (PCS), LCM has to replace the data both in the file and in the RMS-DB following the controlling direction.

8.2. Contents Transaction from LCM to PD

The procedure for a LCM to download a content to its PD follows the below steps:

- LCM requests the PD-ID and UTD data to the PD.
- PD sends the $ENC(CK_{PD\text{-}LCM}, UTD \| PD\text{-}ID)$ to the LCM.
- LCM recovers the PD-ID and confirms it.
- LCM recovers the UTD and SH part compares them with those in its RMS-DB.
- If UTD is correct and if any alteration of RMF is needed, the LCM updates the contents of RMF both in RMS-DB and in the file format.
- LCM updates UTD of RMS-DB by newly generated UTD* and $ENC(CK_{PD\text{-}LCM}, UTD^*)$ is to be sent to the PD.
- If the Transfer Control Status indicates as "Transfer", then replace it by "Transferred" to the Transfer Control Status field in RMS-DB not in the file format. Where the Transfer Control Status field has the three types, "Transfer", Transferred", and "Transfer-non".
- If the Copy Control Status (CCS) indicates "Check-in", then replace it by "Check-out" to the Copy Control Status field both in RMS-DB and in the file format.
- If the Copy Control Status (CCS) indicates "Copy-Never", the content downloading to a PD is denied.
- If any of the above lists does not violate, download the content to the PD.

8.3. Contents Transaction from PD to PM

- For the case that a unique ID of each PM exists :
  For a PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using the unique ID of the PM as an encryption key.

- For the case that a unique ID of each PM does not exist :
  For a PD to write a content on a PM, it just writes the content on the PM and it recovers the Secret Header (SH) and re-encrypts it by using a randomly generated key. Where the randomly generated key, say T, is encrypted by a common secrete key, S (this is a preset value by the manufacturer of the PD), and is also written on a hidden area of the PM.

8.4. Portability of PM

For the first case of the section 8.3, all contents within the PM can be played by all PDs, but, for the second case, all contents within the PM can be played only by the PDs produced by the manufacturers which adopted this system. Any way it is certain that this system can supports the portability of contents via PMs.

8.5. Transferability of a Content

As previously we defined in section 3, the "Transferability" is a different concept from the "Portability" of a content. The main difference is that the content with "Transferability" can be not only played in any PDs but also uploaded to any LCMs, but not in the case of "Portability". Since our system has and manages the Transfer Control Status field both in the RMS-DB and in the file format, our system can support the transferability of a content. If there is marked "Transfer" in the field of a content and if the content is just downloaded to PD, then the LCM downloads it to the PD and replaces "Transfer" by "Transferred" in the relevant field of RMS-DB. Then the content, which has been downloaded to a PD, can no longer be played in the LCM until it is uploaded to the LCM again, but the downloaded content in a PM can be played by any PDs and can be uploaded to another LCM via a PD.

Note : If the Copy Control Status (CCS) of a content contained in a PM indicates "Copy-Free", the content can be uploaded to any LCMs.

9. OUTSOURCE INPUT

As shown in the Fig.9-1, various inputs such as originated from RedBook CD, Audio CD, Super Audio CD, DVD Disk, and analog Device are all allowable to LCM optionally. An analog input to PD is also allowable. The secure import control for those several inputs to LCM or to PD is presented in the next subsections.

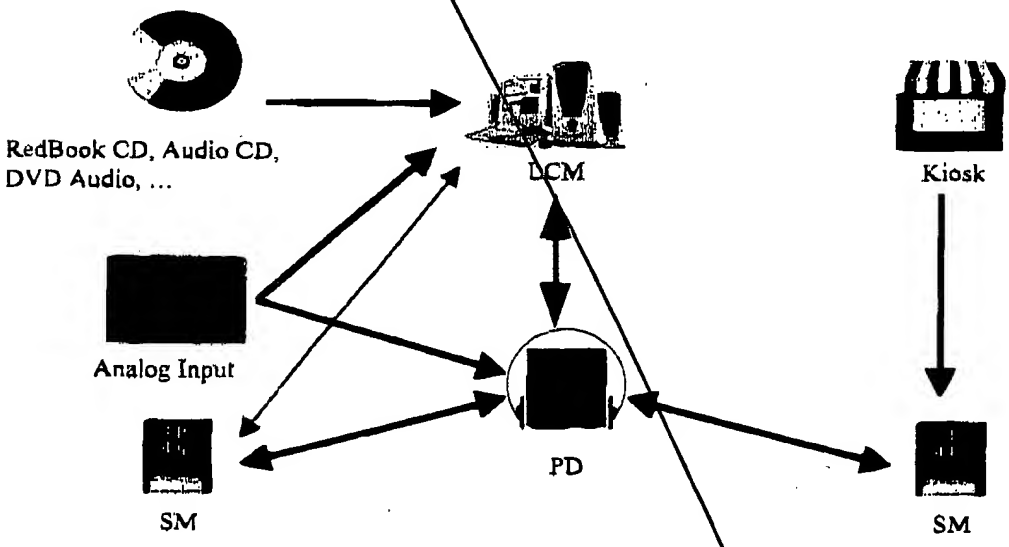


Figure 9-1 : Outsource Input to LCM and PD

9.1. Basic Architecture for a Secure Import Control

As shown in the Fig.9.1-1, the host device, in which the LCM module exists, has at least the following three layers (two of these exist in the LCM module).

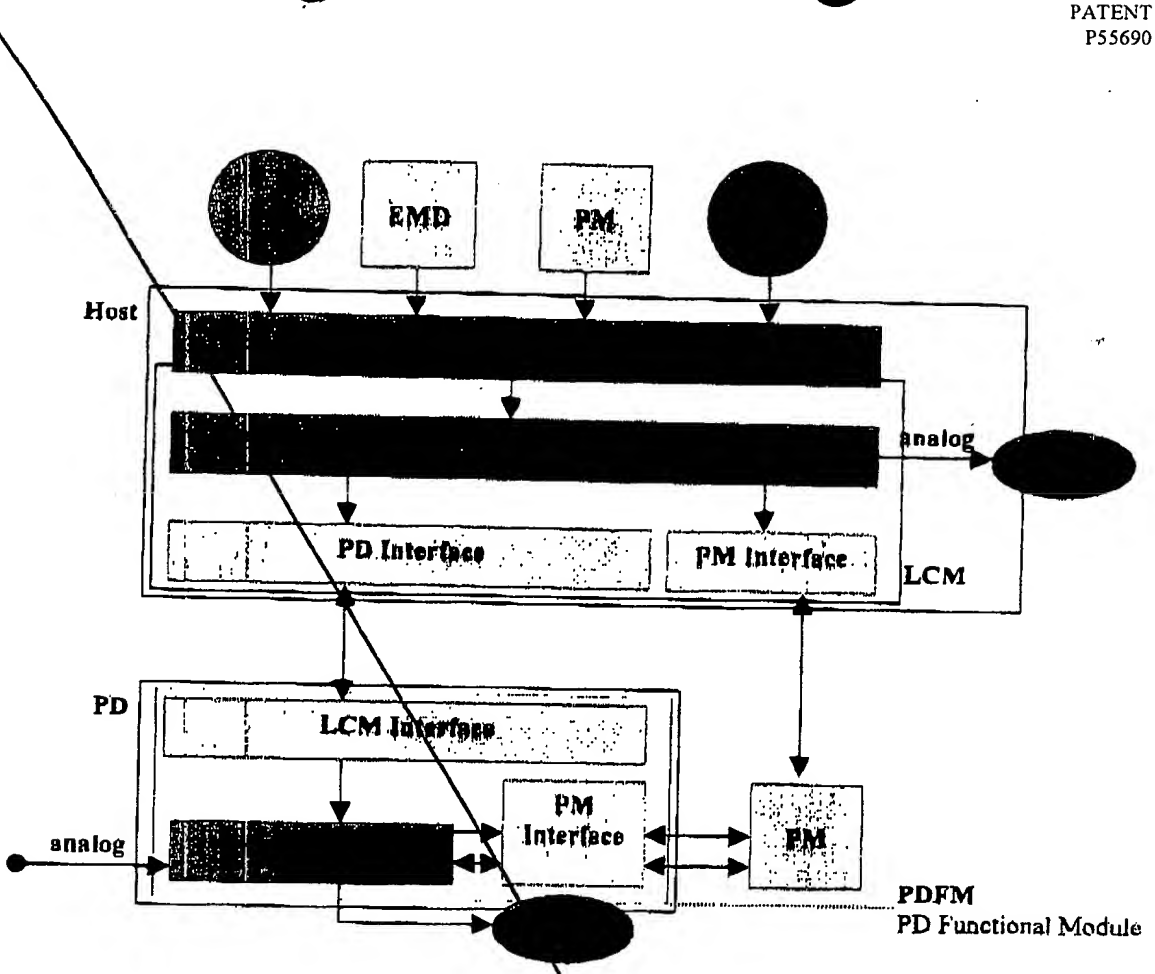


Figure 9.1-1 : Outsource Import Control

- **Authenticated Input API**
  This API has the roles that confirms the validity of the input and extracts some required information to convert the input into a SDMI Compliant format.

  - Validity Check
    - If the input data has a watermark, then this API should be able to detect it.
    - If the input data takes an encrypted (or scrambled) form, then this API should be able to extract its encryption key and the encryption (or scrambling) algorithm.
    - If the input data does not take any protected form, then the API should confirm the validity of written format of the media containing the input data.

  - Required data for the API to pass over to the Import Control Layer.
    - Information of the media (source) type → Audio CD, DVD Audio, ...
    - Information of the originator of the input content
    - Information of the content → Title, if any, Player, Artist, ...
    - Information of the encryption algorithm if any
    - Information of the encryption key if any

- **PD Import Control**

  This Import Control Layer gets a bundle of information from the Authenticated Input API and reconstructs the input content to meet a SDMI Compliant file format by following the rules listed below:

- Copy Control Status → mark "Copy-Never" or "Check-in/Check-out" (optionally)
- Playback Control Status → mark "Times to playback = infinite or N" (N: optional)
- Transfer Control Status → mark "Transfer-Non"
- Mark the "LCM-ID" into the SOI field and Device-ID field of SH(Secret Header)
- If the input content is not encrypted, then generate a random key and encrypt it by the key.
- If the input content takes an encrypted form by other encryption algorithm different from the PD's, then this layer trans-encrypts the content to be played in the PD.
- Public-Key-Encrypt such made secret header part by LCM's public key.

- **PD Interface**

  This layer authenticates the connected PD by checking whether the PD has its correct ID and the secret channel key, $CK_{PD\text{-}LCM}$. Where the Kerberos Authentication Protocol may be used (refer to : A.J. Menezes, P.C. Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, pp.401-403, CRC Press, 1996).

9.2. Analog Input to PD

The Import Control Layer (ICL) within the PDFM makes a SDMI Compliant compressed digital content from the analog input by following the rules listed below:

- Upon reception of each frame of the analog input, the ICL does encoding the frame and does encrypting it by a randomly generated key. If all the frames has been encrypted follow the next steps.
- Copy Control Status → mark "Copy-Never" or "Check-in/Check-out" (optionally)
- Playback Control Status → mark "Times to playback = infinite or N" (N: optional)
- Transfer Control Status → mark "Transfer-Non"
- Mark the "PD-ID" into the SOI field and Device-ID field of SH(Secret Header)
- Encrypt such made secret header part by PD's channel key.

Note : If such converted SDMI Compliant content from the analog input has its SOI field of SH(Secret Header) with marked "PD-ID", then the procedure of writing the content on a PM does not use the unique ID of the PM. → This means that such content as made from an analog input to a PD is not allowed to have the "Portability".

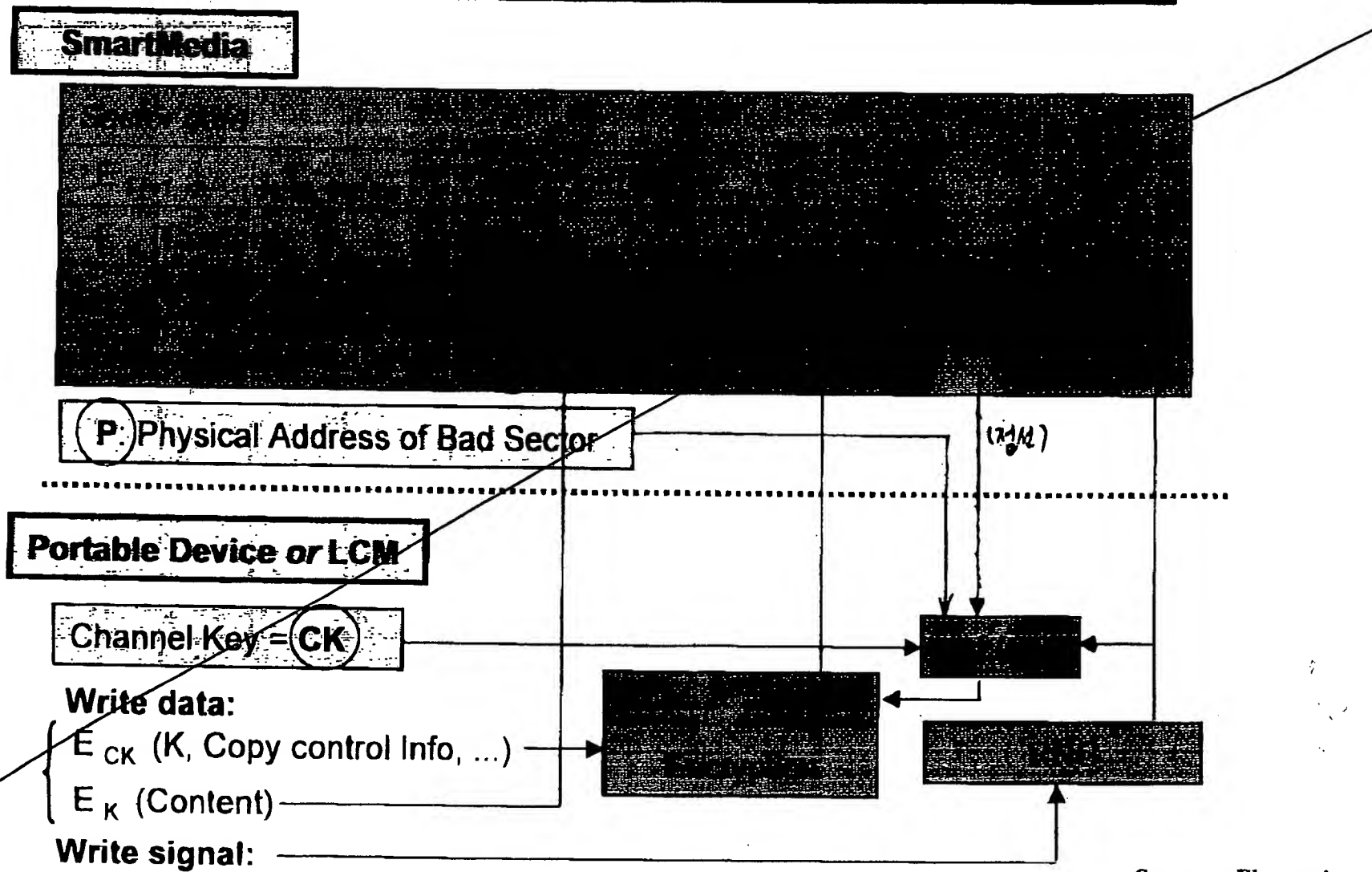
9.3. Kiosk

An example for the "Kiosk" may be a shop or a machine that makes a bundle of SDMI Compliant contents into PMs from CD-Ripping, etc. and sells them. Here we regard such Kiosk-like machine as a special LCM with PM-Interface that has a special contraction with some ISPs and groups of copyright holders. Hence, to make a SDMI Compliant PMs from other physical media, the Kiosk-like machine follows the same routines as described in section 9.1 and 8.3.

10. CONCLUSION

In this article we proposed a secure copy protection mechanism for the Internet based MOD Services. One of our proprietary modules is relevant to the use of and management of MKIT table appeared in the PD registration procedure. Another one is relevant to the construction of secure Check-in/Check-out System which securely maintains the contents downloading /uploading between LCM and PD.

SAMSUNG Copy Protection Scheme for Portable Media



Samsung Electronics

SAMSUNG Copy Protection Scheme for Portable Media

1. Unique ID, ID (Optional feature)

- PM may *optionally* support unique ID for 1st Generation PM.
- If Unique ID is not supported, Physical address of bad sector of PM is used instead.
- If unique ID is supported, it should be one-time writeable during manufacturing stage only, and readable only by PD with a special command.

2. Channel Key, CK

- CK is a shared key between LCM and PD.
- To support portability, CK is not considered as input to function f().
- If CK is included, it provides additional security to the content stored in PM.
- CK may take various forms depending on the application usage and right management rules.

3. Physical Address of Bad Sector of Portable Media, P

- The usage of P prevents the playback of illegally copied content from PM to PM by simple "dead-copy"

4. Spared Area

- A special command known only to the manufacturer needs to be known to access this area.